



DEPARTMENT OF THE ARMY
OFFICE OF THE ASSISTANT SECRETARY
MANPOWER AND RESERVE AFFAIRS
111 ARMY PENTAGON
WASHINGTON, DC 20310-0111

March 26, 2003

MEMORANDUM FOR CHIEF INFORMATION OFFICER/G-6

SUBJECT: Army Information Resources Management Exemption

Reference memorandum, OSA (SAIS-ZR), 21 January 2003, subject: Exemption Request, The Third Wave Initiative.

Function. Army Information Resources Management. The Army Chief Information Officer (CIO)/G-6 has a statutory responsibility to advise and assist the Secretary of the Army to ensure that information resources are managed for the Department of the Army in a manner that implements the Clinger-Cohen Act (CCA), 40 U.S. Code Section 11101 *et. seq.*, consistent with guidance provided by the Secretary of the Army. The Secretary of the Army has provided the CIO/G6 with guidance to implement the CCA in a series of Army Knowledge Management (AKM) Guidance Memoranda. AKM is an integral part of the Army's transformation, and will result in new management structures and a network-centric, knowledge-based workforce. Managing information resources in a network-centric, knowledge-based force constitutes an Army core war-fighting competency. This core competency includes information operations that support operating forces, and utilizes commercial technologies adapted for military applications.

Decision. The Army's Chief Information Officer (CIO)/G-6 is an inherently Governmental position involving the interpretation and execution of United States law, including the CCA and the e-Government Act. The position is mandated by 40 U.S. Code, Section 11315, 44 U.S. Code, Section 3506(a)(2)(B), and 10 U.S. Code 3014 (c)(1)(D) and (2).

The Senior Information Security Officer is an inherently governmental position involving the interpretation and execution of United States law, including the Federal Information Security Management Act of 2002. The position is mandated by 44 U.S. Code, Section 3544. Managing Army information resources is an Army core competency. The functions within this core competency that cannot be divested include: subordinate organizations and personnel through which the CIO/G-6 exercises authority to fulfill his statutory responsibilities; subordinate organizations and personnel

performing information security functions that insure command, control, and communications interoperability across Army, Joint, Interagency, and Coalition forces.

Within this core competency, however, there are functions amenable to outsourcing. In accordance with the CCA, AKM guidance, and this decision memorandum, the Army CIO/G-6 shall promote the effective and efficient design and operation of all major information resources management processes for the Army, including improvements to the Army's work processes, in the following core competency areas:

- Director of Information Management Functions
- Enterprise level help desk services
- Enterprise single sign-on and directory services
- Enterprise server consolidations
- Consolidation of functional processing centers
- Network consolidations

Within TDA organizations, the use of military personnel to perform information resources management functions is limited to the extent required by career progression determinations and rotational base considerations. Within the operating forces, information resources-related functions (including information operations) must be military when Uniform Code of Military Justice (UCMJ) authority is needed in order to compel performance in certain operational situations (e.g. if there is a high likelihood of being ordered to a hostile environment).

With regard to personal services, the exemption is granted to the extent necessary to avoid inappropriate personal services contracts. Enclosed are instructions to implement this decision in the Inventory of Commercial and Inherently Governmental Activities (including the Federal Activities Inventory Reform Act Inventory), to be developed by the Deputy Chief of Staff, G-1 in coordination with responsible staff officers. The limitations and scope of this decision are discussed in detail below.

Requestor's Positions on Issues. Information resources went through considerable outsourcing during the First and Second Wave initiatives. Information resources that remain to be outsourced are being reviewed pursuant to the SECARMY's AKM guidance. The CIO/G-6 is currently developing an outsourcing strategy based on managing the Army "Infostructure" at the enterprise level using best industry practices. The strategy's expected completion time is mid-2003. Efficiencies of roughly 25% are anticipated in the short term as a result of AKM implementation.

This strategy is consistent with the CCA's direction that outsourcing of information resources be delegated to agency CIOs, and it will meet the intent of the Third Wave initiative. Additional efficiencies are anticipated in the out years as a result of Army transformation and Objective Force initiatives.

Standard of Review. The senior HQDA functional official for a function must describe and substantiate specifically how preparation and implementation of a Third Wave implementation plan for each course of action poses substantial and specific risks to a core war-fighting mission of the Army (*i.e.*, a core competency) or violates a statutory requirement affecting a function. The following are the risk factors to evaluate this request: force management risk, operational risk; future challenges; and institutional risk. How these risk criteria are applied may vary based on each course of action evaluated (*i.e.*, A-76; alternatives to A-76; military conversions; transfers to another agency; and divestiture). Therefore, exemption requests and decisions must assess the potentially adverse impact of each course of action.

Risk Issues Relevant to Core Competencies. The Army CIO/G-6 is ultimately responsible for providing Information Superiority over the enemy. Information superiority is a core component of Sustained Land Dominance and enables the other Army core competencies: Shape the Security Environment, Prompt Response, Forcible Entry Operations, Mobilization, and Support Civil Authority (FM-1). Today's organizational structure consists of a strong balance of military and civilian personnel, augmented where appropriate by contractor personnel. Army signal units link deployed forces to their power projection and support platforms (CONUS and OCONUS) and link commanders to the National Command Authority through a 24x7 enterprise network of tactical C2 and strategic business information systems. These missions support the Army's command and control functions. Therefore, there is a force management risk (*i.e.*, career progression) and an operational risk associated with divesting these functions. As noted in the Decision paragraph above, however there are a number of information resource functions that may be best performed by private sector sources from the standpoint of keeping pace with emerging technologies.

Statutory Requirements Relevant to Divestiture. The CCA, 40 U.S. Code, Section 1131, vests responsibility for managing and acquiring information resources with the head of each executive agency. In accordance with 10 U.S. Code, Section 3014(c)(1)(D) and (2), and 44 U.S. Code, Section 3506(a)(2)(B), the Secretary of the Army has designated the Army CIO/G-6 as the single officer responsible for information management within the Office of the Secretary of the Army. In addition, the Federal

Information Security Management Act of 2002, 44 U.S. Code, Sections 3541-49, directs the appointment of a Senior Information Security Officer. The Army CIO/G-6 is in the process of establishing the Army Knowledge Enterprise (AKE), the Army's enterprise-level information resources infrastructure, or "Infostructure." Through the AKE, the CIO/G-6 exerts control and directs activities in a manner that ensures compliance with the CCA, the Federal Information Security Management Act of 2002, and other applicable statutes. Therefore, the functions performed by the CIO/G-6 and Senior Information Security Officer cannot be divested.

Inherently Governmental Functions Relevant to Outsourcing. Inherently Governmental functions include those activities that require either the exercise of substantial discretion in applying Government authority, or making value judgments in making decisions for the Government. An inherently Governmental function is so intimately related to the public interest that a Federal Government employee must perform it.

In order to establish, manage, and secure the AKE, the CIO/G-6 and the Senior Information Security Officer bind the Army to take or not take actions pursuant to the CCA, the Federal Information Security Management Act of 2002, DoD Information Assurance regulations and policies, AKM policies, and other statutes and regulations applicable to managing information resources and information assurance. Moreover, these officials exert ultimate control over acquiring, using, and disposing of the Army's information resources.

Statutes Relevant to Outsourcing. As stated in paragraph (5) above, the CIO/G-6 has specific statutory responsibilities regarding the management of Army information resources. The CIO/G-6 fulfills those responsibilities through the emerging AKE. In order to ensure the AKE is established in a manner that implements those statutes, the CIO/G-6 is responsible for making assessments and recommendations to the Secretary of the Army regarding outsourcing of specific information resources.

Information resources that are commercial but not exempt from outsourcing are subject to 10 U.S. Code, Sections 2461 and 8014 of the 2003 DoD Appropriations Act, mandating public-private competition in certain circumstances (subject to the standard exceptions for 10 or fewer civilian employees, and preferential procurement programs). For these information resources, the CIO/G-6 should follow applicable OMB guidance and DoD regulations and instructions that provide specific outsourcing guidance (*i.e.*, A-76; alternatives to A-76; military conversions; transfers to another agency). There is a basis for exempting that activity, whether advisory or clerical support, to avoid

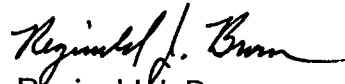
Personal Services. Where supervision by an official required by statute (such as the CIO/G-6) is required to effectively perform an activity in support of that official, is an inappropriate personal services contract. In addition, if personnel supervised by an official must in-turn supervise individuals supporting them in order to effectively perform the activity, a further extension of this exemption may be warranted. In the case of contractors accompanying the operating forces, there also may be a legitimate basis for exempting the function from contractor performance.

Conflicts of Interest. No conflict of interest issues have been presently identified in the referenced exemption request. Conflicts of interest must be avoided through appropriate safeguards in the administration of the contracted work.

Military Conversions. There are significant recruiting and retention challenges associated with growing an in-house capability that retains currency with emerging technologies in the Information Technology (IT) functional area. Real world lessons-learned have shown that because of the tremendous demand for trained IT personnel, contractors also have had a difficult time in maintaining a stable workforce. The DOD Inventory of Commercial and Inherently Governmental Activities Guide contains guidance for risk assessment. Applying the guidelines in paragraph 1-1, use of non-military personnel in combat support roles must be assessed in terms of risk to "the support mission and the missions dependent on that support." Combat mission failure or loss of life are severe risks, while "loss of support elements that augment or enhance operations in theatre during a conflict often have minor impact on combat operations." On today's battlefield, information operations and resources are not merely support elements that augment or enhance operations; rather they are essential to achieving information superiority, which is the key to mission success. Integrated Network Operations (NETOPS) enable the war-fighter to see the Common Operational Picture (COP) and achieve information dominance. When a person is deployed into an environment where refusal to obey a commander's orders would create a risk of loss of life or mission failure, UCMJ authority may be needed to compel performance, thus requiring military incumbency.

Outside of military theater operational areas the central issue concerns whether adequate performance of the (IT) function in the infrastructure requires military unique knowledge and skills. According to the Office of Secretary of Defense Guidance for compiling the Inventory of Commercial and Inherently Governmental Activities, military unique knowledge and experience can only be derived from *recent* first-hand involvement in military activities – i.e., through commanding military forces or conducting or participating in military operations or exercises. This knowledge and

experience must be more substantial than familiarity with doctrine, tactics, operations, or regulations; capabilities that can be developed by civilians; or, advice military retirees can provide based on their knowledge and experiences.



Reginald J. Brown
Assistant Secretary of the Army
(Manpower and Reserve Affairs)

Enclosures

* "Information resources" means information and related resources, such as personnel, equipment, funds, and information technology. 44 U.S. Code, Section 3502(6).

CODING RULES for Information Management

1. Office of the Chief Information Officer (DCS, G6)
 - a. Chief of Information Operation (DCS, G6)
Code F – Military Unique Skills and Knowledge
 - b. Chief of Information Security
Code F – Military Unique Skills and Knowledge
 - c. All military and civilian in W4NJAA
Code L – Protected by law, statute, treaty or agreement
2. Signal Units in the Operating Forces
 - a. All military in SRC11 (Signal Corps) units
Code B – Support to Military Operations
3. Undergoing restructuring in Army Knowledge Management Plan
 - a. All personnel in TDA Augmentations to SRC11 MTOE units
Code P – Pending Restructuring
 - b. OCONUS Regional Centers for Information Operations
 - c. Military Signal Corps in Generating forces
 1. Officers: Branch 25 (Signal), FA24 (Sys Eng), FA30 (Info Sys Ops), FA 53 (Systems Automation)
 2. Warrant: Branch 25 (Signal)
 3. Enlisted: CMF25 (Visual Info), CMF31 (Signal), CMF35 (Electronic Maint), CMF74 (Record Info Ops)
- d. Civilians in key occupational series
 1. GS-332 (Computer Operations)
 2. GS-334 (Computer Specialist)
 3. GS-854 (Computer Engineer)
 4. GS-855 (Electrical Engineer)
 5. GS-2210 (Info Tech Management)

- | | | Code P – Pending Restructuring |
|---|--|--------------------------------|
| 4. Network Security and Telecommunication Centers | | |
| | a. W341AA Army Network Operations Security Center | |
| | b. W341AA CONUS Theatre Network Operations Security Centers | |
| | c. WG8699 Europe Theatre Network Operations Security Centers | |
| | d. WDMA99 Korea Theatre Network Operations Security Centers | |
| | e. WCD099 Pacific Theatre Network Operations Security Centers | |
| | f. WNAJ99 USSOUTHCOM Theatre Network Operations Security Centers | |
| 5. Subject to Review | | Code R – Subject to Review |
| | a. All civilian GS-335 (Computer Clerk/Asst) | |
| | b. All Army personnel in information management not otherwise exempted by this or another decision | |